IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :

Mutsuyuki OKAYAMA et al. : **Attn: BOX PCT**

Serial No. NEW : **Docket No. 2002_0292A**

Filed February 28, 2002 :

COPYRIGHT PROTECTIVE DEVICE AND METHOD
[Corresponding to PCT/JP01/05484
Filed June 27, 2001]

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEE FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975.

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents,
Washington, DC 20231

Sir:

Please amend the above-identified application as follows.

In The Specification:

Please replace the paragraph beginning at page 22, line 24 with the following rewritten paragraph:

FIG. 1 is a block diagram illustrating a structure of a copyright protective device according to the first embodiment of the present invention. The copyright protective device shown in FIG. 1 comprises a key generation section 10, a key information retention/selection section 20, a content encryption/decryption section 30, input registers 40, a heading pattern detector 50, and a reset/input enable signal generation circuit 60. The copyright protective device generates key information K, applies encryption processing or decryption processing to input data DI using the generated key information K, and outputs output data DO. Hereinafter, features of the copyright protective device shown in FIG. 1 will be described in connection with the aforementioned three problems (key generation, output control, and reset/input control).

ATTACHMENT H

Please replace the paragraph beginning at page 40, line 9 with the following rewritten paragraph:

The intermediate keys and final key are stored on a medium in an encrypted fashion. The key generation section 10 first sets the value of a variable n to one (step S101). Note that the variable n is a variable which is used for sequentially processing a plurality of device keys. The plurality of device keys are sequentially labeled as device key A, device key B, device key C, ..., etc., and media keys corresponding to the respective device keys are sequentially labeled as media key A, media key B, media key C, ..., etc. As the variable n is sequentially updated from 1 to 2 to 3, ..., etc., device keys A, B, C, ..., etc., are processed in the alphabetical order and media keys A, B, C, ..., etc., are generated in the alphabetical order.

Please replace the paragraph beginning at page 41, line 22 with the following rewritten paragraph:

If the pattern DB is not obtained by decrypting the verify media key record (NO from step S107), the key generation section 10 selects a conditionally calculate media key record from the media key block stored on the medium, and inputs this to itself (step S108). Next, the key generation section 10 decrypts the data at byte positions 4 to 11 (recording data header) contained in the conditionally calculate media key record with the current media key A (step S109). Next, the key generation section 10 verifies whether or not the data at byte positions 4 to 7 in the decryption result is the pattern DB (step S110). If the decryption result is not the pattern DB, the key generation section 10 returns to step S108. Note that the verification at step S110 is also directed to conditions other than the verification as to whether or not the pattern DB has been obtained. Since the details thereof are described in the aforementioned first to fourth specification manuals, the descriptions thereof are omitted here.

Please replace the paragraph beginning at page 43, line 6 with the following rewritten paragraph:

The key generation section 10 inputs to itself device key B for deciphering media key B (step S102), decrypts an encrypted media key B with device key B (step S104), decrypts a verify media key record with a current media key B (step S106), and if the pattern DB is obtained as a result, regards the current media key B as media key B (step S107).

Please replace the paragraph beginning at page 46, line 5 with the following rewritten paragraph:

Next, the key generation section 10 reads a verify media key record from the media key block recorded on the medium, and inputs this to itself (step S105). Next, using the current media key A_1 which was derived at step S104, the key generation section 10 decrypts the verify media key record (step S106). As described earlier, a result of encrypting the pattern DB with the media key is recorded in the verify media key record . Therefore, if the pattern DB is obtained by decrypting the verify media key record (YES from step S107), the key generation section 10 regards the current media key A_1 at this point as the correct media key, and proceeds to step S114.

Please replace the paragraph beginning at page 46, line 16 with the following rewritten paragraph:

If the pattern DB is not obtained by decrypting the verify media key record (NO from step S107), the key generation section 10 selects a conditionally calculate media key record from the media key block stored on the medium, and inputs this to itself (step S108). Next, the key generation section 10 decrypts the data at byte positions 4 to 11 (recording data header) contained in the conditionally calculate media key record with the current media key A_1 (step S109). Next, the key generation section 10 verifies whether or not the data at byte positions 4 to 7 in the decryption result is the pattern DB (step S110). If the decryption result is not the pattern DB, the key generation section 10 returns to step S108. Note that the verification at step S110 is also directed to conditions other than the verification as to whether or not the pattern DB has been obtained. Since the details

thereof are described in the aforementioned first to fourth specification manuals, the descriptions thereof are omitted here.

Please replace the paragraph beginning at page 53, line 10 with the following rewritten paragraph:

FIG. 14 is a timing chart of input signals from the copyright protective device according to the present embodiment. In FIG. 14, input signals to the content encryption/decryption section 30 are D0, D1, D2, ..., etc., and output signals from the content encryption/decryption section 30 are d0, d1, d2, ..., etc. It is assumed that the key generation period notification signal GEN shifts to the H level during key generation.

REMARKS

Kindly enter the above editorial corrections prior to initial examination.

Attached hereto is a marked-up version of the changes made to the specification by the current amendment. The attachment pages are captioned "**Version With Markings to Show Changes Made.**"

Respectfully submitted,

Mutsuyuki OKAYAMA et al.

By _____
Charles R. Watts
Registration No. 33,142
Attorney for Applicants

CRW/lah
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
February 28, 2002

protective device according to the eighth embodiment of the present invention.

FIG. 17 is a block diagram for explaining an output control function of a copyright protective device according to a variant of the eighth embodiment of the present invention.

FIG. 18 is a block diagram for explaining an input control function of a copyright protective device according to a ninth embodiment of the present invention.

FIG. 19 is a timing chart of input signals to a copyright protective device according to the ninth embodiment of the present invention.

FIG. 20 is a block diagram for explaining a reset/input control function of a copyright protective device according to a tenth embodiment of the present invention.

FIG. 21 is a block diagram for explaining an input control function of a copyright protective device according to an eleventh embodiment of the present invention.

FIG. 22 is a block diagram for explaining a reset/input control function of a copyright protective device according to a variant of the eleventh embodiment of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

(first embodiment)

FIG. 1 is a block diagram illustrating a structure of a copyright protective device according to the first embodiment of

the present invention. The copyright protective device shown in FIG. 1 comprises a key generation section 10, a key information retention/selection section 20, a content encryption/decryption section 30, input registers 40, a heading pattern detector ~~section~~ 50, and a reset/input enable signal generation circuit 60. The copyright protective device generates key information K, applies encryption processing or decryption processing to input data DI using the generated key information K, and outputs output data DO. Hereinafter, features of the copyright protective device shown in FIG. 1 will be described in connection with the aforementioned three problems (key generation, output control, and reset/input control).

First, a first feature, i.e., reduction of key generation time will be described. FIG. 2 is a block diagram of a key generation section 10. In FIG. 2, the key generation section 10 comprises an intermediate key processing section 11 and a final key processing section 12. FIG. 3 is a block diagram illustrating a structure of the key information retention/selection section 20. In FIG. 3, the key information retention/selection section 20 comprises a selection circuit 21 and a register circuit 22.

In order to facilitate the understanding of the present embodiment, the key generation in a DVD recording/reproduction device will be described as an example. The key generation algorithm illustrated below employs device key A, media key A, media unique key A, title key A, and contents key A. Each

the descriptions thereof are omitted here.

According to CPRM, media key A and media unique key A are employed as intermediate keys, and title key A is generated as a final key. According to CPPM, media key A is employed as an intermediate key, and album unique key A is generated as a final key.

Hereinafter, with reference to FIG. 10, a processing procedure by the key generation section 10 will be described.

The intermediate keys and final key are stored on a medium in an encrypted fashion. The key generation section 10 first sets the value of a variable n to one (step S101). Note that the variable n is a variable which is used for sequentially processing a plurality of device keys. The plurality of device keys are sequentially labeled as device key A, device key B, device key C, ..., etc., and media keys corresponding to the respective device keys are sequentially labeled as media key A, media key B, media key C, ..., etc. As the variable n is sequentially updated from 1 to 2 to 3, ..., etc., device keys A, B, C, ..., etc., are processed in the alphabetical order and media keys A, B, C, ..., etc., are generated in the alphabetical order.

Next, device key A for decrypting an encrypted media key A is inputted to the key generation section 10 (step S102). Note that device key A may be inputted in an encrypted fashion. In this case, the key generation section 10 internally decrypts device key A. Next, the encrypted media key A is inputted to the

key generation section 10 (step S103). More specifically, the key generation section 10 reads, from the media key block recorded on the medium, encrypted key information corresponding to a row and a column which are assigned to device key A. Next, the key generation section 10 decrypts the encrypted media key A with device key A, thereby obtaining media key A (step S104). However, since the media key thus obtained has not been finalized as media key A at this point, this media key is referred to as a current media key A. In order to obtain a finalized media key A, the key generation section 10 further performs the following processing.

Next, the key generation section 10 reads a verify media key record from the media key block recorded on the medium, and inputs this to itself (step S105). Next, using the current media key A which was derived at step S104, the key generation section 10 decrypts the verify media key record (step S106). As described earlier, a result of encrypting the pattern DB with the media key is recorded in the verify media key record. Therefore, if the pattern DB is obtained by decrypting the verify media key record (YES from step S107), the key generation section 10 regards the current media key A at this point as the correct media key, and proceeds to step S114.

If the pattern DB is not obtained by decrypting the verify ~~key-media~~ media key record (NO from step S107), the key generation section 10 selects a conditionally calculate media key record from the media key block stored on the medium, and inputs this to itself

(step S108). Next, the key generation section 10 decrypts the data at byte positions 4 to 11 (recording data header) contained in the conditionally calculate media key record with the current media key A (step S109). Next, the key generation section 10 verifies whether or not the data at byte positions 4 to 7 in the decryption result is the pattern DB (step S110). If the decryption result is not the pattern DB, the key generation section 10 returns to step S108. Note that the verification at step S110 is also directed to conditions other than the verification as to whether or not the pattern DB has been obtained. Since the details thereof are described in the aforementioned first to fourth specification manuals, the descriptions thereof are omitted here.

If the decryption result is the pattern DB, the key generation section 10 refers to the decrypted column information (which is recorded at byte position 8 in the recording data header), regards a device key having that column information as device key B, extracts recording data corresponding to the row information of device key B (step S111), and decrypts it with the current media key A (step S112). This means that the recording data, which has been subjected to a twofold encryption, is decrypted at step S112 with respect to one of the encryptions. Next, the key generation section 10 adds one to the variable n (step S113), and returns to step S102.

If the key generation section 10 returns to step S102, the key generation section 10 applies similar processing to the device

key which was obtained at step S111. However, since the encrypted current media key B has already been inputted as the encrypted intermediate key at step S112, the key generation section 10 does not perform the process of step S103 in the second round of processing or later.

The key generation section 10 inputs to itself device key B for deciphering media key B (step S102), decrypts an encrypted media key B with device key B (step S104), decrypts a verify media key ~~media~~ record with a current media key B (step S106), and if the pattern DB is obtained as a result, regards the current media key B as media key B (step S107).

If the result of verification at step S107 is correct, the current media key is regarded as the correct media key. The key generation section 10 performs computation processing between the derived media key and a media identifier (Media ID), thereby deriving a media unique key (or an album unique key in the case of CPPM). The key generation section 10 decrypts an encrypted title key with the media unique key, and outputs the derived title key to the content encryption/decryption section 30 as a final key K. In the case of CPPM, the key generation section 10 outputs an album unique key, instead of a title key, to the content encryption/decryption section 30 as a final key K.

At step S114 and later, the key information retention/selection section 20 operates. If the variable n is 1 (YES from step S114), the key information retention/selection

obtained has not been finalized as media key A_1 at this point, this media key is referred to as a current media key A_1. In order to obtain a finalized media key A_1, the key generation section 10 further performs the following processing.

Next, the key generation section 10 reads a verify media key ~~media~~ record from the media key block recorded on the medium, and inputs this to itself (step S105). Next, using the current media key A_1 which was derived at step S104, the key generation section 10 decrypts the verify media key ~~media~~ record (step S106). As described earlier, a result of encrypting the pattern DB with the media key is recorded in the verify media key ~~media~~ record . Therefore, if the pattern DB is obtained by decrypting the verify media key ~~media~~ record (YES from step S107), the key generation section 10 regards the current media key A_1 at this point as the correct media key, and proceeds to step S114.

If the pattern DB is not obtained by decrypting the verify media key record (NO from step S107), the key generation section 10 selects a conditionally calculate media key record from the media key block stored on the medium, and inputs this to itself (step S108). Next, the key generation section 10 decrypts the data at byte positions 4 to 11 (recording data header) contained in the conditionally calculate media key record with the current media key A_1 (step S109). Next, the key generation section 10 verifies whether or not the data at byte positions 4 to 7 in the decryption result is the pattern DB (step S110). If the decryption result

is not the pattern DB, the key generation section 10 returns to step S108. Note that the verification at step S110 is also directed to conditions other than the verification as to whether or not the pattern DB has been obtained. Since the details thereof are described in the aforementioned first to fourth specification manuals, the descriptions thereof are omitted here.

If the decryption result is the pattern DB, the key generation section 10 refers to the decrypted column information (which is recorded at byte position 8 in the recording data header), regards a device key having that column information as device key A_2, extracts recording data corresponding to the row information of device key A_2 (step S111), and decrypts it with the current media key A_1 (step S112). This means that the recording data, which has been subjected to a twofold encryption, is decrypted at step S112 with respect to one of the encryptions. Next, the key generation section 10 adds one to the variable n (step S113), and returns to step S102.

If the key generation section 10 returns to step S102, the key generation section 10 applies similar processing to the device key which was obtained at step S111. However, since the encrypted current media key A_2 has already been inputted as the encrypted intermediate key at step S112, the key generation section 10 does not perform the process of step S103 in the second round of processing or later.

The key generation section 10 inputs to itself device key

signal GEN which is outputted from the key generation section 10 is inputted to the output switching switch 37. When the signal GEN is inactive (i.e., not during key generation), the output switching switch 37 selects an output signal (a in FIG. 13) from the content encryption/decryption section 30 for output. On the other hand, when the signal GEN is active (i.e., during key generation), the output switching switch 37 selects an input signal (b in FIG. 13) to the content encryption/decryption section 30 for output.

FIG. 14 is a timing chart of input signals ~~to~~ From the copyright protective device according to the present embodiment. In FIG. 14, input signals to the content encryption/decryption section 30 are D0, D1, D2, ..., etc., and output signals from the content encryption/decryption section 30 are d0, d1, d2, ..., etc. It is assumed that the key generation period notification signal GEN shifts to the H level during key generation.

When the signal GEN is inactive, the output switching switch 37 selects the output signal from the content encryption/decryption section 30 for output. Accordingly, data such as d7, d8, d9, ..., etc., are outputted from the copyright protective device. On the other hand, when the signal GEN is active, the output switching switch 37 selects the input signal to the content encryption/decryption section 30 and outputs it as it is. Accordingly, data from D0 to D7 are outputted from the copyright protective device.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING SUBMISSION OR TRANSMITTAL OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

OGASAWARA, Shiro
Daisan-Longev'Bldg., 3-11, Enokicho
Suita-shi, Osaka 564-0053
JAPON

Date of mailing (day/month/year)	IMPORTANT NOTIFICATION
24 October 2001 (24.10.01)	
Applicant's or agent's file reference: PCT01-052	
International application No.: PCT/JP01/05484	International filing date (day/month/year): 27 June 2001 (27.06.01)
International publication date (day/month/year): Not yet published	Priority date (day/month/year): 29 June 2000 (29.06.00)
Applicant: MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.

3. An **asterisk**(*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

4. The **letters "NR"** appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
29 June 2000 (29.06.00)	2000-196080	JP	17 Augu 2001 (17.08.01)
05 July 2000 (05.07.00)	2000-203375	JP	21 Sept 2001 (21.09.01)
05 July 2000 (05.07.00)	2000-203376	JP	21 Sept 2001 (21.09.01)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
Magda BOUACHA

Telephone No. (41-22) 338.83.38

ATTACHMENT I